



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/663,892	09/18/2000	Robert Chojnacki	N0065US	4139

37583 7590 04/30/2004

NAVIGATION TECHNOLOGIES
222 MERCHANDISE MART
SUITE 900, PATENT DEPT.
CHICAGO, IL 60654

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 04/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/663,892

Applicant(s)

CHOJNACKI, ROBERT

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 September 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 September 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2,3,4.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 15 is objected to because of the following informalities:

(1) A word "date" appeared in line 3 of claim 15 is incorrect. The correct word should be "data". Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-16, 18-32, and 34-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Schneck et al. (US 6,314, 409).

a. Referring to claim 1:

i. Schneck teaches:

(1) establishing an authorization key that defines (i) verification information indicative of at least one authorized entity and (ii) a cryptographic key to the data product [i.e., referring to Figure 1, authoring mechanism 112, that is for "establishing an authorization key ". In addition, Schneck also discloses using the authoring mechanism 112, those elements of the data 106 that are to be encrypted are selected, as are the cryptographic algorithms and protocols to be employed, the payment procedures for the use of the data, and other decisions governing how the user 104 will be permitted to use the data; and employs asymmetric encryption algorithms in the authoring and access mechanisms. The keys for these algorithms are protected within the system and are never exposed (column 12, lines 4-16)];

(2) encrypting the authorization key, thereby producing an encrypted authorization key that can be decrypted using a decryption key [i.e., **executable software-based cryptography can ensure that data are distributed only to authorized users. The information to be protected is encrypted and transmitted to the authorized user(s). Separately, a decryption key is provided only to authorized users. The key is subsequently used to enable decryption of the information so that it is available to the authorized user(s) (column 3, lines 37-44)]**]; and

(3) providing the encrypted authorization key to a system that (i) has access to the decryption key and can therefore decrypt the encrypted authorization key and (ii) is programmed to decrypt the authorization key and to use the verification information to validate use of the data product [i.e., **referring to Figure 1, authoring mechanism, that is for “providing the encrypted authorization key”, to access mechanism, which includes all cryptographic keys, that allows a user 104 to access the data in packaged data 108 (or 150) according to the rules provided with (or separately from, as packaged rules 152) the packaged data and prevents the user or anyone else from accessing the data other than as allowed by the rules. Furthermore, the access mechanism 114 used by the user 104 to access data is described with reference to FIG. 8 and includes a processing unit 154, read-only memory (ROM) 156, volatile memory (RAM) 158, I/O controller 165 and some form of energy source 166 such as, for example, a battery. Access mechanism 114 may also include electrically-alterable non-volatile memory 160, a hard disk 162, a display 164, and special purpose components such as encryption hardware 168 (column 15, lines 31-49)]**].

b. Referring to claim 2:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

c. Referring to claim 3:

i. Schneck further teaches:

(1) wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the system, to determine whether the system is authorized to use the data product [i.e., referring to **Figure 3**, wherein the rules include various forms of validity checking and identification information such as version number 127, authentication data 128, license number 130, intellectual property identifier 132, first and last valid generations of the product 134, 136. The rules 116 further include an encrypted data key 138 as well as the actual rules 140, 142, 144-146 to be applied when access is made to the data by a user. The actual rules include, but are not limited to, standard, extended and custom permissions 140, 142, 144-146, and co-requisite rules (permission lists) of source data 145 (column 11, lines 5-15)].

d. Referring to claim 4:

i. Schneck further teaches:

(1) wherein the predetermined information associated with the system comprises a system ID [i.e., referring to **Figure 3**, the function of each field in the rules shown in **Figure 3** is given in **TABLE I**, which includes **System IDs/Public key 147** (column 11, lines 20-48)].

e. Referring to claim 5:

i. Schneck further teaches:

(1) wherein providing the encrypted authorization key to the system comprises sending the encrypted authorization key to the system via a wireless communications network [i.e., the data 106 provided to the distributor 102 and the packaged data 108 (or 150 and packaged rules 152, if provided separately) provided to the user 104, may be provided and distributed in various ways, including but not limited to, via digital communications networks (for example, the Internet or the projected National Information Infrastructure (NII)), magnetic media (for example, tape or disk), CD-ROM, semiconductor memory modules (for example, flash memory, PCMCIA RAM cards), and wireless (for example, broadcast) (column 15, lines 10-19)].

f. Referring to claim 6:

i. Schneck further teaches:

(1) wherein providing the encrypted authorization key to the system comprises recording the encrypted authorization key on a data storage medium and then providing the data storage medium to the system [i.e., the access mechanism 114, which includes all cryptographic keys, used by the user 104 to access data is described with reference to FIG. 8 and includes a processing unit 154, read-only memory (ROM) 156, volatile memory (RAM) 158, I/O controller 165 and some form of energy source 166 such as, for example, a battery. Access mechanism 114 may also include electrically-alterable non-volatile memory 160, a hard disk 162 (for recording the encrypted authorization key on a data storage medium and then providing the data storage medium to the system), a display 164, and special purpose components such as encryption hardware 168 (column 15, lines 41-49)].

g. Referring to claim 7:

i. This claim has limitations that is similar to those of claims 1 and 6, thus it is rejected with the same rationale applied against claims 1 and 6 above.

h. Referring to claim 8:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

i. Referring to claim 9:

i. Schneck further teaches:

(1) wherein the predetermined information associated with the data storage medium comprises a data storage medium ID [i.e., the distributor 102 includes storage (in which storage ID is inherently provided) means for storing the rules and/or predetermined information (column 7, lines 26-27)].

j. Referring to claim 10:

i. Schneck further teaches:

(1) wherein the data product comprises a database of geographic information [**i.e., this system can be used to ensure privacy of sensitive records in a database. Examples include financial, census, medical, and political databases and the like, wherein “a database of geographic information” is considered to include in this database (column 32, lines 23-25)].**

k. Referring to claim 11:

i. Schneck further teaches:

(1) assembling a set of authorization parameters associated with the data; computing a first checksum of the set of authorization parameters; generating a first cryptographic key substantially randomly; using the first cryptographic key to symmetrically encrypt the set of authorization parameters, so as to produce an encrypted set of authorization parameters; encrypting a combination of the first cryptographic key and the first checksum, so as to produce a header value that can be decrypted using a second cryptographic key; and providing the header value, together with the data, for access by a receiving end [**i.e., referring to Figure 1, the authoring mechanism 112 is for “assembling a set of authorization parameters associated with the data; computing a first checksum of the set of authorization parameters; generating a first cryptographic key substantially randomly; using the first cryptographic key to symmetrically encrypt the set of authorization parameters, so as to produce an encrypted set of authorization parameters; encrypting a combination of the first cryptographic key and the first checksum, so as to produce a header value that can be decrypted using a second cryptographic key; and providing the header value, together with the data, for access by a receiving end” (column 11, line 56 through column 15, line 29)].**

l. Referring to claim 12:

i. Schneck further teaches:

(1) using the second cryptographic key to decrypt the header value, so as to produce an decrypted header value; retrieving the first cryptographic key and first checksum from the decrypted header value; using the first cryptographic key to decrypt the encrypted set of authorization parameters; computing a

second checksum of the set of authorization parameters; comparing the second checksum with the first checksum, and refusing to access the data if the second checksum does not match the first checksum; and using the set of authorization parameters to verify authorization to access the data [i.e., referring to Figure 1, the **distribution mechanism 118 is for “using the second cryptographic key to decrypt the header value, so as to produce an decrypted header value; retrieving the first cryptographic key and first checksum from the decrypted header value; using the first cryptographic key to decrypt the encrypted set of authorization parameters; computing a second checksum of the set of authorization parameters; comparing the second checksum with the first checksum, and refusing to access the data if the second checksum does not match the first checksum; and using the set of authorization parameters to verify authorization to access the data” (column 11, line 56 through column 15, line 29)].**

m. Referring to claim 13:

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

n. Referring to claim 14:

i. Schneck further teaches:

(1) assembling an authorization key that includes verification information indicative of a data storage medium on which the data is authorized to be stored [i.e., referring to Figure 5, a distributor 102, that is for **“assembling an authorization key that includes verification information indicative of a data storage medium on which the data is authorized to be stored”**. Furthermore, the distributor 102 also includes storage means for storing the rules (column 7, lines 26-27)]; and

(2) encrypting the authorization key and the data, thereby producing an encrypted authorization key and encrypted data [i.e., **executable software-based cryptography can ensure that data are distributed only to authorized users. The information to be protected is encrypted and transmitted to the authorized user(s). Separately, a decryption key is provided only to**

authorized users. The key is subsequently used to enable decryption of the information so that it is available to the authorized user(s) (column 3, lines 37-44)];

(3) storing the encrypted authorization key and encrypted data on a given data storage medium [i.e. referring to Figure 1, access mechanism 114 may also include electrically-alterable non-volatile memory 160, a hard disk 162, that is for “storing the encrypted authorization key and encrypted data on a given data storage medium” (column 15, lines 41-49)]; and

(4) thereby providing the given data storage medium to a system that is programmed to decrypt the authorization key and to determine, by reference to the verification information whether the given storage medium is the data storage medium on which the data is authorized to be stored [i.e., referring to Figure 1, authoring mechanism, that is for “providing the encrypted authorization key”, to access mechanism, which includes all cryptographic keys, that allows a user 104 to access the data in packaged data 108 (or 150) according to the rules provided with (or separately from, as packaged rules 152) the packaged data and prevents the user or anyone else from accessing the data other than as allowed by the rules. Furthermore, the access mechanism 114 used by the user 104 to access data is described with reference to FIG. 8 and includes a processing unit 154, read-only memory (ROM) 156, volatile memory (RAM) 158, I/O controller 165 and some form of energy source 166 such as, for example, a battery. Access mechanism 114 may also include electrically-alterable non-volatile memory 160, a hard disk 162, a display 164, and special purpose components such as encryption hardware 168 (column 15, lines 31-49)].

o. Referring to claim 15:

i. Schneck further teaches:

(1) the system decrypting the encrypted data only if the verification information indicates that the given storage medium is the data storage medium on which the data is authorized to be stored [i.e., the information to be protected is encrypted and transmitted to the authorized user(s). Separately, a

decryption key is provided only to authorized users. The key is subsequently used to enable decryption of the information so that it is available to the authorized user(s) (column 3, lines 37-44)].

p. Referring to claim 16:

i. This claim has limitations that is similar to those of claims 1, 11, and 12, thus it is rejected with the same rationale applied against claims 1, 11 and 12 above.

q. Referring to claims 18 and 34:

i. These claims have limitations that is similar to those of claims 9 and 10, thus they are rejected with the same rationale applied against claims 9 and 10 above.

r. Referring to claim 19:

i. Schneck further teaches:

(1) wherein the first function comprises a hash function **[i.e., the function of each field in the rules shown in Figure 3 is given in TABLE I, which includes Authentication (hash) 128 (column 11, lines 16-25)].**

s. Referring to claim 20:

i. Schneck further teaches:

(1) wherein the input parameters further include a predetermined segment of the encrypted portion of the data product **[i.e., the function of each field in the rules shown in Figure 3 is given in TABLE I, which includes Co-requisite rules (permissions) for source data 145, that is for “predetermined segment of the encrypted portion of the data product” (column 11, lines 16-39)].**

t. Referring to claims 21-27, 37-38:

i. These claims have limitations that is similar to those of claim 16, thus they are rejected with the same rationale applied against claim 16 above.

u. Referring to claim 28:

i. Schneck further teaches:

(1) randomly generating the first cryptographic key **[i.e., the encryption of the data stored on the hard disk can use cryptographic keys**

generated within the access mechanism and which are never known outside of the mechanism (column 17, lines 12-15)].

v. Referring to claim 29:

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

w. Referring to claim 30:

i. Schneck further teaches:

(1) wherein the portion of the data product comprises information required to understand contents of the data product **[i.e., a protected dataset (packaged data) read by a system which does not employ an access mechanism 114 according to the present invention (or a dataset read by a system in non-protected mode) will be treated as data without any decryption taking place (by an access mechanism). In such a system, protected data elements will not be available to the user (column 21, lines 20-25)].**

x. Referring to claim 31:

i. Schneck further teaches:

(1) wherein the information required to understand contents of the data product is selected from the group consisting of (i) database decompression information and (ii) pointers **[i.e., referring to Figure 3, the function of each field in the rules shown in Figure 3 is given in TABLE I, whereby "database decompression information and pointers" are considered to include in this TABLE I (column 11, lines 16-39)].**

y. Referring to claim 32:

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

z. Referring to claim 35:

i. This claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

aa. Referring to claim 36:

i. This claim has limitations that is similar to those of claim 20, thus it is rejected with the same rationale applied against claim 20 above.

ab. Referring to claim 39:

i. Schneck teaches:

(1) a processor; a data storage medium; and a set of machine language instructions, stored in the data storage medium and executable by the processor to carry out the method steps of claim 27 [i.e., referring to Figure 8, The access mechanism 114 used by the user 104 to access data is described with reference to FIG. 8 and includes a processing unit 154, read-only memory (ROM) 156, volatile memory (RAM) 158, I/O controller 165 and some form of energy source 166 such as, for example, a battery. Access mechanism 114 may also include electrically-alterable non-volatile memory 160, a hard disk 162, a display 164, and special purpose components such as encryption hardware 168 (column 15, lines 41-49). Furthermore, Program execution occurs when a computer device follows a series of steps, or instructions, expressed in some symbology. The program may be linear, with one step always following its predecessor without variation, or the program may involve branching based on comparison of variables related to internal or external events and status. In the field of computer science a distinction is sometimes made according to the time at which the instructions comprising the program are translated into the computer's machine language in order to control the operation of the computer. Accordingly, terms such as assembly, compilation, and interpretation are used. This distinction is not important with respect to the present invention. The term execution is used herein to refer to all forms of program execution (column 24, lines 33-47)].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

Art Unit: 2135

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 17 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneck et al, and further in view of Brunts et al (US 5, 887, 2699).

a. Referring to claims 17 and 33:

i. Schneck teaches all the claimed subject matter except for:

(1) applying with a navigation system.

ii. However, Brunts teaches:

(1) a system and method are provided for allowing access to authorized data information for use in a data access system. The invention is particularly suited for use with a navigation system for offering navigational assistance to a mobile user. Data information, such as destination-related information for navigational services, could be made available to a user with an authorization code encrypted within the data. Available reading devices, such as navigation systems, are assigned authorization identification codes, from a large pool of possible codes, preferably so that each system has its own identification number. The data information is provided to a user so that the data has a data identification code which coincides with the identification code for his or her reading device. Additionally, a user could create a data card authorized for a given reading device by using the corresponding authorization identification code (**column 3, lines 41-56**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) apply the navigation system with the system using encryption method for controlling access and distribution of digital property (in Schneck) in order to secure the protection of rights to data and information (**column 1, lines 15-16 of Schneck**).

iv. The ordinary skilled person would have been motivated to:

(1) apply the navigation system with the system using encryption method for controlling access and distribution of digital property (in Schneck)

because without the tamper detection/reset mechanism of this invention, software can be modified or data can be intercepted rendering useless any attempts at control (column 7, lines 6-10 of Schneck).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

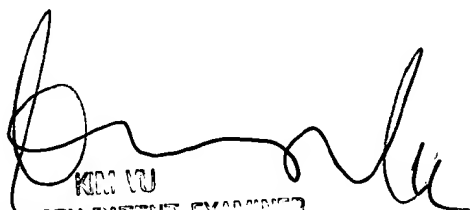
a. Dowling et al (US 6, 522, 875) discloses a geographical web browser allows a user to navigate a network application such as the Word Wide Web by physically navigating in geographical coordinates. For example, a geographical web browser is implemented in a mobile unit such as a dashboard computer (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
April 22, 2004


KIM VU
SUPERVISOR, PATENT EXAMINER
TECHNOLOGY CENTER 2100